Насоки за сертифицирање на информацискиte системи

1. За кого е наменет документот

Овој документ е наменет за министерствата, другите органи на државната управа, организациите утврдени со закон и други државни органи, судовите, јавните обвинителства и државното правобранителство, правни и други лица кои со закон им е доверено да вршат јавни овластувања, органите на општините, на градот Скопје и на општините на градот Скопје, што разменуваат или се должни да разменуваат податоци и документи во електронска форма, односно остварување на административни услуги по електронски пат, кога тоа е утврдено согласно законот за електронско управување. Документот ќе се ажурира согласно потребите.

2. Вовед

Врз основа на член 36 од Законот за електронско управување, Министерството за информатичко општество и администрација ги сертифицира информацискиte системи кои ги користат органите за комуникација за електронски пат и го пропишува начинот на сертифицирање, како и формата и содржината на сертификатот.

Согласно член 6 од Правилникот за начинот на сертифицирање на информацискиte системи кои ги користат органите за комуникација по електронски пат, како и за формата и содржината на сертификатот за функционалност на информацискиte системи, министерството за информатичко општество и администрација подготви "Насоки за сертифицирање на информацискиte системи".

По утврдување на исполнетоста на условите за сертифицирање на информацискиот систем, согласно член 4 од Правилникот за начинот на сертифицирање на информацискиte системи кои ги користат органите за комуникација по електронски пат министерството за информатичко општество и администрација издава *сертификат* за функционалност на информацискиот систем.

3. Податоци што се потребни

Барањето за сертификација на информацискиte системи кои ги користат органите за комуникација по електронски пат согласно правилниците на законот за електронско управување ги содржи следните елементи:

- назив и седиште на органот,
- податоци кои го идентификуваат информацискиот систем (модел, верзија и конфигурација на составните софтверски и хардверски компоненти) и

- опфат на информациските систем кој ги вклучува документите и податоците во електронска форма,

а кон барањето се приложува потребната документација за утврдување на податоците и техничката документација за информациските систем.

4. Начин на сертифицирање на информациските системи

1. Државниот орган утврдува за кои од информациските системи кои ги користи за комуникација по електронски пат согласно закон е потребно да достави барање за сертификација до Министерството за информатичко општество и администрација, односно го утврдува опфатот и податоците кои го идентификуваат информацискиот систем како и целта на сертифицирањето – приклучување на нов систем на системот за размена на документи и податоци, промена на постоечки систем и други ситуации утврдени со закон.

2. Државниот орган доставува барање за сертификација, за секој информциски систем посебно, до Министерството за информатичко општество и администрација, Сектор за интероперабилност. Електронската верзија на образецот *Барање за добивање сертификат* (прилог 1) е објавен на веб локацијата на министерството.

   Пополнетото барање за добивање сертификат се доставува во писмена форма и во електронска форма на sertifikati@mioa.gov.mk.

3. Министерството за информатичко општество и администрација или правно лице од областа за која се издава сертификатот определено од страна на Министерството, ја утврдува исполнетоста на условите за сертифицирање на информацискиот систем (прилог 2).

   Државниот орган обезбедува пристап до целосниот систем и потребните документи за системот кој е предмет за сертификација, обезбедувајќи услови за непречена работа на лицата кои ќе вршат проверка на исполнетоста на условите.

   Министерството за информатичко општество и администрација подготвува овластувања за сите лица кои ќе ја вршат проверката на условите и за тоа го известува државниот орган. Сите лица кои ќе бидат вклучени во проверката ќе потпишат *Изјава за взаемна доверливост на податоци* (прилог 4).

➢ Доколку органот изврши промени на информацискиот систем или информацискиот систем престанал да ги исполнува горенаведените услови службено во писмена форма или електронски, доставува известување до Министерството.

4. Министерството за информатичко општество и администрација издава сертификат за функционалност на информацискиот систем доколку се

исполнети бараните услови и за тоа го известува државниот орган, а во случај дел од условите да не се исполнети или по елаборирана препорака од лицата кои ја вршеле проверката, Министерството доставува допис до државниот орган за условите кои треба да се исполнат за да се издаде сертификат.

5. Министерството за информатичко општество и администрација води евиденција во електронска форма на издадените сертификати за функционалност на информациските системи.

   Евиденцијата на сертификатите за функционалноста на информациските системи потребно е да ги содржи следните рубрики:

   - реден број;
   - архивски број и датум на поднесување на барањето за добивање на сертификат;
   - назив и седиште на органот кој е подносител на барањето;
   - број и датум на издаден сертификат за функционалност на информацискит систем и рок на негова важност;
   - податоци кои го идентификуваат информацискиот систем, како модел, верзија и конфигурација на составните софтверски и хардверски компоненти;
   - опфат на информацискиот систем, кој ги вклучува документите и податоците во електронска форма кои ги обработуваат преку системот;
   - број и датум на новиот издаден сертификат за функционалност на информацискиот систем;
   - број и датум на решението за престанување на важноста на претходно издадениот сертификат;
   - забелешка;

4.1. Пополнување на барање за сертификација

Електронскиот образец (прилог 1) е во форма на формулар кој треба да се пополни. За секое поле што треба да го пополни државниот орган има дадено соодветно објаснување.

За достава по електронска пошта, се користат следните параметри:

Електронска пошта (e-mail) на примач: sertifikati@mioa.gov.mk
Предмет (Subject): Baranje_za_sertifikacija_[akronim od nazivot na institucijata]
Пополнетиот образец се праќа како прилог (attachment) на пораката.
Во пораката се содржани контакт податоците на испраќачот на пораката и истите мора да се согласни со адресата од која се испраќа пораката, односно пораките кои ќе бидат пратени од комерцијални сервери за електронска пошта не се земаат на разгледување.

БАРАЊЕ ЗА СЕРТИФИКАЦИЈА

на функционалност на информациски систем

Назив на органот:	[*Назив на органот кој е подносител на известувањето]*
Седиште на органот:	[*Седиште на органот кој е подносител на известувањето]*
Информациски систем:	[*Назив на информацискиот систем кој треба да се сертифицира]*
Модел:	[Модел на *информацискиот систем кој треба да се сертифицира]*
Верзија:	[Верзија на *информацискиот систем кој треба да се сертифицира]*
Опсег на информацискиот систем кој треба да се сертифицира	[*Опис на*: - *инфраструктура* - *хардверски елементи* - *софтверски елементи* - *функционалности (услуги)* - *мрежа* - *човечки ресурси* - *податоци (регистрирани бази на податоци)* - *други елементи релевантни за сертификацијата*]

Во прилог на барањето е доставена следната документација потребна за утврдување на податоците наведени погоре, вклучувајќи ја и техничката и друга потребна документација од значење на информацискиот систем кој ќе се сертифицира:

1. ____
2. ____

Датум _____ Подносител на барањето

_____ _____

УСЛОВИ ЗА СЕРТИФИКАЦИЈА

на функционалност на информациски систем

Забелешка: За сите барања означени со (*) во крајната десна колона, потребно е да се обезбеди документација.

1.	**Технички барања, начин на работа и функционирање на комуникацискиот клиент**	
1.1.	*Технички барања во однос на хардверската и софтверската инфраструктура на комуникацискиот клиент*	
1	За хардверската опрема се обезбедени физичките услови според спецификацијата на производителот:	(*)
а	соодветна температура	
б	електрично напојување	
в	просторни услови	
г	има физичко обезбедување на просторот каде што е поставена опремата	
2	Назначени се лица на позициите:	(*)
а	мрежен администратор	
б	системски администратор	
1.2.	*Технички барања за размена на податоци и документи*	
1	Институцијата/ органот поседува активна интернет конекција	(*)
2	Во рамки на органот се користат веб прелистувачи или специфични клиентски апликации кои дозволуваат меѓу другото и директен пристап до Интернет базирани сервиси, сервери за електронска пошта и други ресурси	
3	Адресите на електронската пошта на јавната и државната администрацијата е во поддомејните на домејнот на Владата на РМ "gov.mk"	
4	Институцијата за обезбедување на административни услуги по електронски пат има можност за размена на пораки по електронска пошта користејќи сметки од службена електронска пошта	
5	При користење на безбедносни сертификати и директориумски услуги се користи X.500 сетот на стандарди	(*)
6	За безбедна размена на податоци преку протоколите: HTTP, LDAP, FTP и други	
7	За шифрирање на XML пораки се користи XMLENC	

2.	**Барања за Информацискиот систем кој поседува електронски регистар**	
2.1.	Назначени се лица на позициите:	(*)
а	администратор за база на податоци	
б	ИТ персонал за одржување и поддршка	
2.2.	Воспоставени се процедури за:	(*)

а	правење на резерни копии	
б	одржување и ажурирање на податоците во регистрите	
2.3.	Воспоставени се параметри за пребарување на податоците со цел идентификација на поединечни записи	
2.4.	Можност за конверзија на податоците од електронскиот регистар во податоци со XML формат	

3.	**Барања за оценка и управување на ризикот**	
3.1.	Органот има воспоставено структуриран пристап во управувањето со ризиците	(*)
3.2.	Процесот за управување со ризиците опфаќа:	(*)
а	оценка на големина	
б	избор на ефективни и економски мерки за нивно намалување	
в	спроведување на ефективни и економски мерки за нивно намалување	
г	оценка дали преостанатите (резидуалните) ризици се во прифатливи граници	
3.3.	Процесот за управување со ризиците ги вклучува следниве фази:	(*)
а	избор на објектите кои ќе бидат предмет на анализа	
б	избор на методологија за оценка на ризикот	
в	идентификација на информациските средства	
г	откривање на слабостите/ранливоста на информацискиот систем / средства	
д	анализа на заканите и можните последици од нив	
ѓ	оценка на ризиците	
е	избор на заштитни мерки	
ж	реализација и проверка на ефикасноста и ефективноста на избраните мерки	
з	оценка на преостанатиот (резидуалниот) ризик	
3.4.	Органот спроведува проценка и оценка на ризиците по однос на безбедноста на информацискиот систем	(*)

4.	**Барања за доверливоста на информациите и нивоата на пристап до нив**
Нивоата на заштита од неовластен пристап до информациите во информациските системи на органите се следните: ниво "0" или "D" - ниво на слободен пристап; ниво "1" или "C" - ниво на слободно управување на пристап; ниво "2" или "B" - ниво на принудно управување на пристап; ниво "3" или "A" - ниво на голема безбедност.	
Забелешки: Зависно од нивоата на доверливост на информациите барањата се 4.1, 4.2, 4.3 и 4.4.за ниво “0”, “1”, “2” и “3” соодветно. Исполнетоста на барањата за доверливост на информациите и нивоата на пристап до нив се утврдува за сите нивоа на информации кои се опфатени со инфомацискиот систем кој	

се сертифицира.		
4.1.	Информациите се јавни и општо достапни	
4.2.	За пристап до информациите се применуваат следните основни мерки:	(*)
а	корисниците се идентификуваат, пред да можат да преземат било каква акција – автентикација	
б	за докажување на идентитетот се користи заштитен механизам од типот корисничко име/лозинка, без дополнителни проверки за основните податоци на корисникот	
в	пристапот до точно определени информации е пропишан на точно определени корисници – авторизација	
г	воспоставена е доверлива комуникација помеѓу корисниците и системот со користење на криптографски протоколи	
д	информациите кои се користат за докажување на идентитетот на корисниците кои пристапуваат во системот се заштитени од неовластен пристап	
ѓ	системот за контрола на пристап функционира самостојно, заштитен од надворешни влијанија и од обиди да се следи текот на неговата работата	
е	информацискиот систем располага со технички и/или програмски средства, со кои ќе може периодично да се проверува валидноста на системот за контрола на пристап	
ж	заштитните механизми имаат поминато тест, којшто ќе потврди дека корисникот нема можност да ги заобиколи и да добие неовластен пристап до информациите кои тие ги штитат	
4.3.	За пристап до информациите се применуваат мерките од 4.2. и дополнително следните мерки:	(*)
а	како механизам за проверка на идентитетот на корисниците се користи електронски потпис	
б	независно дали е издаден за употреба во локалната инфраструктура на јавен клуч во рамките на конкретниот орган, или е издаден од надворешен доставувач на доверливи услуги	
в	при издавање на електронски потпис органот дополнително ги проверува основните податоци за корисникот, без да е потребно негово лично присуство	
г	воспоставена е доверлива комуникација помеѓу корисниците и системот преку VPN или протоколите SSL или TLS	
д	доверливиот информациски систем обезбедува реализација на принудно управување на пристапот до сите објекти, според претходно строго дефинирани правила на пристап	
ѓ	доверливиот информациски систем обезбедува взаемна изолација на процесите преку разделување на адресниот простор	
4.4.	За пристап до информациите се применуваат мерките од 4.2. и 4.3. дополнително следните мерки:	(*)
а	како механизам за идентификација да се користи електронски потпис издаден од владина инфраструктура на јавен клуч	
б	при издавање на електронскиот потпис направена е физичка потврда за идентитет на лицето	
в	за остварување на заштитена размена на пораки по протоколите	

	HTTP, LDAP, FTP и други, се користи протокол TLS или VPN решенија за безбедносно криптирање на сесиите	
г	за криптирање на XML базирани пораки на ниво на сесија се користи протоколот XMLENC	
д	доверливиот информациски систем не дозволува намалување на неговата безбедност како резултат на долготрајни обиди за нејзино нарушување	
ѓ	доверливиот информациски систем има механизми за регистрација на обидите за нарушување на неговата безбедност	

5.	**Барање за следење и управување на инциденти поврзани со информациска безбедност**	
5.1.	Организиран и воспоставен е центар за управување со инциденти поврзани со информацискатa безбедност (CERT тим), вклучувајќи и развиени формални процедури за следење и управување со безбедносни инциденти.	(*)
5.2.	Процесот за управување со информациско - безбедносни инциденти ги вклучува следните елементи:	(*)
а	откривање на инцидентот	
б	единствена точка за пријавување	
в	евидентирање	
г	доделување на приоритет на инцидентот и негова класификација	
д	проценка на настанот/инцидентот и одлука за начинот на справување со него	
ѓ	обновување дефинирање на прво ниво за решавање на инциденти и услови за пренасочување на друго повисоко ниво	
е	верификација и затворање на инцидентот	
ж	идентификација на потребни подобрувања на процедурите за справување со безбедносни инциденти	
з	следење на инцидентите и управување со нивниот животен циклус	
5.3.	Правилата за управување со безбедносни инциденти (подготвени од CERT тимот) ги содржат следните елементи:	(*)
а	список на идентификувани важни функции на системот и приоритетите за обновување на функционалностите на системот	
б	список на идентификувани ресурси кои се неопходни за исполнување на критично важните функции	
в	список на можните инциденти со веројатности за нивно појавување, произлегувајќи од оценките на ризикот	
г	разработени стратегии за обновување на функционалноста на системот	
д	дефинирани мерки за реализација на стратегиите	
5.4.	Идентификувани се ресурсите кои е потребно да се резервираат за обновување на функциите на системот, и тоа: *Забелешка: Органите зависно од потребите може да користат и комбинација од овие правила, со исклучок на правилото утврдено во алинејата 2 кое е задолжително.*	(*)
а	паралелно запишување или огледална репликација на чуваните	

	податоци	
б	формиран центар за обновување по инциденти, во кој се извршува постојано архивско чување на информациите од системот	
в	резервни ресурси на критичните оперативни функции на примарниот систем кои ќе бидат во состојба да ја превземат функционалноста доколку се случи пад на системот	
5.5.	Воспоставувена е процедура со која при евидентирањето на настаните и инцидентите се создаваат и чуваат најмалку следните записи:	(*)
а	датум и време на случување на настанот	
б	единствен идентификатор на корисникот	
в	тип на настанот	
г	резултат од настанот	
д	извор на настанот	
ѓ	список на засегнатите објекти	
е	опис на измените во системот кои произлегуваат од настанот	

ПРИЛОГ 3

ЗАПИСНИК ОД ИЗВРШЕН СЛУЖБЕН УВИД

Архивски бр. _____

Дата: ___/____/_____

Република Македонија
Министерство за информатичко општество и администрација

бул."Св.Кирил и Методиј", бр.54
1000 Скопје,
Република Македонија
Тел. (02) 3200 870

Факс. (02) 3221 883

Е-пошта: contact_mis@mis.gov.mk
Сајт: www.mioa.gov.mk

Врз основа на поднесеното барање за сертификација од _____ со број _____, Министерството за информатичко општество и администрација изврши увид на информацискиот систем наведен во барањето.

Увидот беше реализиран од [датум] до [*датум*], од страна на [*име и презиме*], [*име и презиме*] и [...]. При увидот на самото место се утврди фактичката состојба на информацискиот систем:

_____

_____

Од извршениот увид утврдено е неисполнување на следните ставки: _____.

Согласно наодите од извршениот увид се констатира дека се/не се исполнети условите за сертифицирање на информацискиот систем, согласно Законот за електронско управување и прописите донесени врз основа на овој закон.

Записникот е изработен во четири (4) истоветни примероци, два (2) за Министерството за информатичко општество и администрација и два (2) за органот кој поднел барање за сертификација на информациски систем.

Министерство за информатичко општество и администрација - службено лице	Овластено лице на органот каде е извршен увидот
_____	_____

ПРИЛОГ 4

Архивски бр. _____

Дата: ___/____/_____

Република Македонија
Министерство за информатичко општество и администрација

бул."Св.Кирил и Методиј", бр.54
1000 Скопје,
Република Македонија
Тел. (02) 3200 870

Факс. (02) 3221 883

Е-пошта: contact_mis@mis.gov.mk
Сајт: www.mioa.gov.mk

ИЗЈАВА

ЗА ВЗАЕМНА ДОВЕРЛИВОСТ НА ПОДАТОЦИ

Сите документи, спецификации, софтвер или податоци за него, оперативни или технички информации, независно дали се дадени во писмена, вербална или електронска форма од било која договорна страна која открива свои доверливи податоци (која понатаму во постапката за сертифицирање ќе се вика „Давател на податоци“) на друга договорна страна (која понатаму во постапката за сертифицирање ќе се вика „Примател на податоци“) во врска со постапката за сертифицирање на информациските системи на органот, и кои информации се заштитени на или се сметаат за доверливи од Давателот на податоците и кои, како такви се обележани како доверливи или заштитени или се соопштени во доверба од страна на Давателот на податоците, ќе се сметаат за Доверливи Информации согласно со закон, а нивното користење и чување "Примателот на податоци" ќе го врши врз основа на оваа изјава и согласно со закон.

„Давател на податоци“ „Примател на податоци“

_____ _____